REMARKS

The present application was filed on September 15, 2005, with claims 1-40. The present application claims priority to PCT application US04/21846, filed July 9, 2004, and U.S. provisional application Serial No. 60/486,127, filed July 10, 2003. Claims 1-40 remain pending in the present application.

Claim 3 is objected to under 37 CFR 1.75(c) as being in improper dependent form.

Claims 1, 2, 6, 14, 16, 19, 37 and 39 are rejected under 35 U.S.C. §102(b) as being anticipated by chapter 12 of Menezes et al., "Handbook of Applied Cryptography." (hereinafter "Menezes").

Claims 3-5 and 8 are rejected under 35 U.S.C. §103(a) as being unpatentable over Menezes.

Claims 13, 35, 36, 38 and 40 are rejected under 35 U.S.C. §103(a) over Menezes in view of Official Notice.

Claims 7, 9-12, 15, 17, 18 and 20-34 are rejected under 35 U.S.C. §103(a) over Menezes in view of one or more other cited references.

With regard to the 37 CFR 1.75(c) objection, although Applicants traverse for at least the reasons identified in Applicants' previous response, Applicants have nonetheless chosen to amended claim 3 without prejudice solely in order to expedite prosecution by conforming to the subjective preference of the Examiner. Support for the amendment to claim 3 may be found in the specification at, for example, page 6, lines 30-32; page 7, line 31, to page 8, line 2; and page 8, lines 13-17. Applicants respectfully submit that the present amendment merely complies with a requirement of form expressly set forth in the present Office Action at page 3, lines 1-4, without requiring further search or consideration by the Examiner. Accordingly, Applicants respectfully request entry of the present amendment under 37 CFR 1.116(b)(1).

With regard to the §102 rejection, the Federal Circuit has recently reiterated that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. §102." *Net MoneyIN Inc. v. VeriSign Inc.*, 545 F.3d 1359, 1369, 88 USPQ2d 1751, 1759 (Fed. Cir. 2008).

Applicants respectfully traverse on the ground that Menezes fails to teach all of the limitations arranged or combined in the same way as recited in the independent claims. By way of example, independent claim 1 specifies an arrangement in which a seed generation client and a seed generation server each independently generate a seed as a function of at least a first string, which is provided by the seed generation server to the seed generation client, and a second string. generated by the seed generation client and sent to the seed generation server.

Applicants respectfully note that the portion of Menezes relied upon by the Examiner in rejecting claim 1 in fact describes two distinct types of key update techniques: key transport techniques, described within §12.3.1(i), and key derivation techniques, described within §12.3.1(ii).

As described in Menezes at page 8, first paragraph, key transport techniques involve "transfer of a specific key chosen *a priori* by one party." Thus, Menezes' key transport techniques involve generation of a key by one party and transfer of that key to the other party. As described in Menezes at page 9, last paragraph, "[k]ey update may be achieved by key transport as above, or by *key derivation* wherein the derived session key is based on per-session random input provided by one party."

In formulating the rejection of claim 1, the Examiner combines Menezes' teachings on page 9 regarding key transport techniques in which a session key can be computed as a function of inputs from both parties (i.e., of r_A and r_B), but in which the session key is not independently generated by the two parties, with Menezes' disclosure on page 10 of a key derivation technique in which both parties compute the session key as a function of only r_B.

The Federal Circuit has expressly stated that "it was error . . . to find anticipation by combining different parts of the separate protocols in [a] reference simply because they were found within the four corners of the document." *Net MoneyIN Inc.*, 545 F.3d at 1369, 88 USPQ2d at 1760. Thus, the Examiner's combination of different parts of the separate protocols taught by Menezes in order to reach the limitations of claim 1 cannot sustain a §102 rejection.

In view of the foregoing, Applicants respectfully assert that Menezes fails to disclose any technique in which a seed generation client and a seed generation server each independently generate a seed as a function of at least a first string and a second string of the type recited in claim 1. Accordingly, Menezes fails to anticipate claim 1.

Although the present rejection of claim 1 is under §102 rather than §103, Applicants also submit that claim 1 is not rendered obvious by Menezes. As discussed in *KSR International Co. v. Teleflex Inc.*, 127 S.Ct 1727, 1741, 82 USPQ2d 1385, 1396 (U.S. 2007), a "patent composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art." In particular, "when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious." *Id.*, 127 S.Ct at 1740, 82 USPQ2d at 1395 (citing *United States* v. *Adams*, 383 U.S. 39, 51-52, 148 USPQ 479, 484 (1966)). Applicants respectfully submit that not only does Menezes fail to suggest that it would be obvious to combine aspects of a key transport technique and a key derivation technique in the manner proposed by the Examiner, but Menezes in fact teaches directly away from any such combination by describing these techniques as distinct alternatives to one another. See, e.g., Menezes at page 2 ("Key establishment may be broadly subdivided into *key transport* and *key agreement*. . . . Additional variations beyond key transport and key agreement exist, including various forms of *key update*, such as *key derivation* in §12.3.1").

Independent claims 35-40 include limitations similar to those discussed above with regard to claim 1, and are believed allowable for reasons similar to those outlined above in the context of claim 1.

Applicants note that, in rejecting independent claims 35, 36, 38 and 40, the Examiner relies on Official notice to supplement Menezes so as to reach the limitations of said claims. As discussed in MPEP 2144.03(A), "it is never appropriate to rely solely on official notice regarding 'common knowledge' in the art, without evidentiary support in the record, as the principal evidence upon which a rejection was based." Rather, "specific knowledge of the prior art must always be supported by citation to some reference work recognized as standard in the pertinent art." *Id.*; see also *In re Eynde,* 480 F.2d 1364, 1370, 178 USPQ 470, 474 (CCPA 1973) ("[W]e reject the notion that judicial or administrative notice may be taken of the state of the art.")

Applicants respectfully submit that the conclusory statements proffered by the Examiner in rejecting claims 35, 36, 38 and 40 fail to satisfy these requirements. Accordingly, Applicants respectfully request that, for each invocation of official notice, the Examiner provide either documentary evidence or an affidavit or declaration setting forth specific factual statements and explanation to support the finding, as required by 37 CFR 1.104(d)(2) in order for such a

rejection to be maintained. Furthermore, Applicants respectfully submit that, even if permissible, the Examiner's invocation of Official notice fails to remedy the above-noted deficiencies of Menezes with regard to the limitations discussed above with reference to claim 1.

Dependent claims 2-34 are believed allowable at least by virtue of their dependence from claim 1, and are also believed to define separately-patentable subject matter. For example, the invocation of official notice in rejecting dependent claim 13 is believed to be inappropriate for reasons similar to those discussed above with regard to independent claims 35, 36, 38 and 40. Likewise, the additional references cited by the Examiner in rejecting claims 7, 9-12, 15, 17, 18 and 20-34 fail to supplement the fundamental deficiencies of the Menezes reference as applied to claim 1.

In view of the foregoing, claims 1-40 are believed to be in condition for allowance.

Respectfully submitted,

/joseph b. ryan/

Date: February 15, 2011

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517